1. An electronic transaction system, comprising a blind auditable membership proof that enables a user to establish that the user knows a value associated with a token in a non-secret membership list of tokens associated with values.

2. The system of claim 1, wherein transactions occurring in the system can be monitored and audited.

3. The system of claim 2, wherein the user remains fully anonymous.

4. The system of claim 3, wherein the token is non-transferable.

5. The system of claim 1, wherein the token can be invalidated.

6. The system of claim 1, wherein the membership lists is distributed to at least one of the party with whom the user transacts and a public database.

7. The system of claim 6, wherein an issuer of the token cannot be forced to issue tokens that cannot be invalidated later.

8. An electronic transaction system, comprising:
an issuer of a token for use in a transaction;
a blind auditable membership proof that enables a user to establish that the user knows a value associated with a token in non-secret membership list that includes tokens associated with values; and
a transacting party which verifies that the user knows an auditable membership proof for the token.

9. The system of claim 8, wherein the user remains anonymous to the transacting party.

10. The system of claim 8, wherein the tokens are non-transferable.

11. The system of claim 10, wherein the tokens can be invalidated.

12. The system of claim 8, wherein the security of the system does not depend on the maintenance of a secret key

13. The system of claim 12, wherein the security of the system relies on the integrity of public data.

14. A method for determining whether to accept a token in connection with a transaction, comprising:

receiving from a user an electronic token;

verifying that the user knows a blind auditable membership proof for the token,

wherein the blind auditable membership proof establishes that the user knows a value associated with some token in non-secret membership list of tokens associated with values; and

accepting the token upon successful verification.

15. The method of claim 14, wherein the verification step does not reveal information from which the user's identity can be determined.

16. The method of claim 14, wherein the membership list is maintained by an issuer of the token.

17. The method of claim 16, wherein the issuer transmits information associated with updated membership lists to at least one of the party with whom the user transacts and a public database.

18. The method of claim 14, further comprising the step of removing the value associated with a token from the membership list.

19. The method of claim 14, wherein the verification step further comprises use of membership proofs combined with zero knowledge proofs.

20. The method of claim 19, wherein the verification step further comprises use of hash chains.

21. The method of claim 20, further comprising the step of monitoring and auditing transactions associated with the token.

22. An electronic payment method, comprising:

verifying that a user knows a blind auditable membership proof for a coin, wherein the blind auditable membership proof establishes that the user knows a value associated with a coin in a non-secret membership list of coins associated with values;

receiving a request to pay electronic coins to a merchant; and

crediting an account of the merchant in an amount of the electronic coin upon successful verification.

23. A computer program product, tangibly stored on a computer-readable medium, for determining whether to accept a token in connection with a transaction, comprising instructions operable to cause programmable processors to:

receive from a user an electronic token;

verify that the user knows a blind auditable membership proof for the token, wherein the blind auditable membership proof establishes that the user knows a value associated with some token in non-secret membership list of tokens associated with values; and

accept the token upon successful verification.

24. The computer program product of claim 23, wherein the instructions do not require the user to reveal information from which the user's identity can be determined.

25. The computer program product of claim 23, wherein the membership list is maintained by an issuer of the token.

26. The computer program product of claim 23, further comprising instructions operable to cause programmable processors to transmit information associated with updated membership lists to at least one of the party with whom the user transacts and a public database.

27. The computer program product of claim 26, further comprising instructions operable to cause programmable processors to remove the value associated with a token from the membership list.

28. The computer program product of claim 26, further comprising instructions operable to cause programmable processors to verify the user's a user knows a blind auditable membership proof.

29. The computer program product of claim 28, further comprising instructions operable to cause programmable processors to verify that a user knows a blind auditable membership proof through a hash chain.

30. The computer program product of claim 23, further comprising instructions operable to cause programmable processors to monitor and audit transactions associated with the token.

31. A computer program product, tangibly stored on a computer-readable medium, for determining whether to accept an electronic coin as payment, comprising instructions operable to cause programmable processors to:

verify that a user knows a blind auditable membership roof for a coin, wherein the blind auditable membership proof establishes that the

user knows a coin associated with a value in a non-secret membership list;

receive a request to pay electronic coins to a merchant; and

credit an account of the merchant in an amount of the electronic coin upon successful verification.